CLAIMS

What is claimed is:

1. A method for authorizing access to controlled resources within a distributed data processing system, the method comprising:

receiving an attribute certificate from a client at a host within the distributed data processing system;

extracting a first locator from the attribute certificate, wherein the first locator identifies a location of a public key certificate of an issuing authority for the attribute certificate;

retrieving the public key certificate of the issuing authority for the attribute certificate;

verifying the attribute certificate using the public key certificate of the issuing authority for the attribute certificate; and

authorizing the client to have access to the controlled resources in accordance with authorization attributes stored in the attribute certificate.

2. The method of claim 1 further comprising:

extracting a second locator from the attribute certificate, wherein the second locator identifies a location of a public key certificate of a holder of the attribute certificate;

retrieving the public key certificate of the holder of the attribute certificate;

authenticating the holder using the public key certificate of the holder.

3. The method of claim 1 wherein the attribute certificate and the public key certificate of the issuing authority for the attribute certificate are formatted according to the X.509 standard.

4. The method of claim 1 wherein the first locator is stored within an X.509 extension within the attribute certificate.

5. A method for obtaining authorized access to controlled resources within a distributed data processing system, the method comprising:

sending an attribute certificate from a client to a host within the distributed data processing system, wherein the attribute certificate comprises a first locator that identifies a location of a public key certificate of an issuing authority for the attribute certificate; and

receiving authorization for the client to access the controlled resources in accordance with authorization attributes stored in the attribute certificate.

6. The method of claim 5, wherein the attribute certificate comprises a second locator that identifies a location of a public key certificate of a holder of the attribute certificate, further comprising:

receiving authentication for a holder of the attribute certificate.

7. A method for generating a digital certificate, the method comprising:

receiving, at an attribute-certificate-issuing authority, a request for an attribute certificate from a client;

generating the attribute certificate in response to the received request for an attribute certificate, wherein the attribute certificate comprises a first locator that identifies a location of a public key certificate of the attribute-certificate-issuing authority; and

sending the generated attribute certificate to the client.

8. The method of claim 7 further comprising:

retrieving from the request for an attribute certificate a second locator that identifies a location of a public key certificate of a subsequent holder of the attribute certificate; and

embedding in the attribute certificate the second locator.

9. An apparatus for authorizing access to controlled resources within a distributed data processing system, the apparatus comprising:

receiving means for receiving an attribute certificate from a client at a host within the distributed data processing system;

first extracting means for extracting a first locator from the attribute certificate, wherein the first locator identifies a location of a public key certificate of an issuing authority for the attribute certificate;

first retrieving means for retrieving the public key certificate of the issuing authority for the attribute certificate;

verifying means for verifying the attribute certificate using the public key certificate of the issuing authority for the attribute certificate; and

authorizing means for authorizing the client to have access to the controlled resources in accordance with authorization attributes stored in the attribute certificate.

10. The apparatus of claim 9 further comprising:

second extracting means for extracting a second locator from the attribute certificate, wherein the second locator identifies a location of a public key certificate of a holder of the attribute certificate;

second retrieving means for retrieving the public key certificate of the holder of the attribute certificate;

authenticating means for authenticating the holder using the public key certificate of the holder.

11. The apparatus of claim 9 wherein the attribute certificate and the public key certificate of the issuing authority for the attribute certificate are formatted according to the X.509 standard.

12. The apparatus of claim 9 wherein the first locator is stored within an X.509 extension within the attribute certificate.

13. An apparatus for obtaining authorized access to controlled resources within a distributed data processing system, the apparatus comprising:

sending means for sending an attribute certificate from a client to a host within the distributed data processing system, wherein the attribute certificate comprises a first locator that identifies a location of a public key certificate of an issuing authority for the attribute certificate; and

first receiving means for receiving authorization for the client to access the controlled resources in accordance with authorization attributes stored in the attribute certificate.

14. The apparatus of claim 13, wherein the attribute certificate comprises a second locator that identifies a location of a public key certificate of a holder of the attribute certificate, further comprising:

second receiving means for receiving authentication for a holder of the attribute certificate.

15. An apparatus for generating a digital certificate, the apparatus comprising:

receiving means for receiving, at an attribute-certificate-issuing authority, a request for an attribute certificate from a client;

generating means for generating the attribute certificate in response to the received request for an attribute certificate, wherein the attribute certificate comprises a first locator that identifies a location of a public key certificate of the attribute-certificate-issuing authority; and

sending means for sending the generated attribute certificate to the client.

16. The apparatus of claim 15 further comprising:

retrieving means for retrieving from the request for an attribute certificate a second locator that identifies a location of a public key certificate of a subsequent holder of the attribute certificate; and

embedding means for embedding in the attribute certificate the second locator.

17. A computer program product in a computer readable medium for use in a distributed data processing system for authorizing access to controlled resources within the distributed data processing system, the computer program product comprising:

instructions for receiving an attribute certificate from a client at a host within the distributed data processing system;

instructions for extracting a first locator from the attribute certificate, wherein the first locator identifies a location of a public key certificate of an issuing authority for the attribute certificate;

instructions for retrieving the public key certificate of the issuing authority for the attribute certificate;

instructions for verifying the attribute certificate using the public key certificate of the issuing authority for the attribute certificate; and

instructions for authorizing the client to have access to the controlled resources in accordance with authorization attributes stored in the attribute certificate.

18. The computer program product of claim 17 further comprising:

instructions for extracting a second locator from the attribute certificate, wherein the second locator identifies a location of a public key certificate of a holder of the attribute certificate;

instructions for retrieving the public key certificate of the holder of the attribute certificate;

instructions for authenticating the holder using the public key certificate of the holder.

19. The computer program product of claim 17 wherein the attribute certificate and the public key certificate of the issuing authority for the attribute certificate are formatted according to the X.509 standard.

20. The computer program product of claim 17 wherein the first locator is stored within an X.509 extension within the attribute certificate.

21. A computer program product in a computer readable medium for use in a distributed data processing system for obtaining authorized access to controlled resources within the distributed data processing system, the computer program product comprising:

instructions for sending an attribute certificate from a client to a host within the distributed data processing system, wherein the attribute certificate comprises a first locator that identifies a location of a public key certificate of an issuing authority for the attribute certificate; and

instructions for receiving authorization for the client to access the controlled resources in accordance with authorization attributes stored in the attribute certificate.

22. The computer program product of claim 21, wherein the attribute certificate comprises a second locator that identifies a location of a public key certificate of a holder of the attribute certificate, further comprising:

instructions for receiving authentication for a holder of the attribute certificate.

23. A computer program product in a computer readable medium for use in a data processing system for generating a digital certificate, the computer program product comprising:

instructions for receiving, at an attribute-certificate-issuing authority, a request for an attribute certificate from a client;

instructions for generating the attribute certificate in response to the received request for an attribute certificate, wherein the attribute certificate comprises a first locator that identifies a location of a public key certificate of the attribute-certificate-issuing authority; and

instructions for sending the generated attribute certificate to the client.

24. The computer program product of claim 23 further comprising:

instructions for retrieving from the request for an attribute certificate a second locator that identifies a location of a public key certificate of a subsequent holder of the attribute certificate; and

instructions for embedding in the attribute certificate the second locator.

25. A data structure representing an attribute certificate for use in a data processing system, the data structure comprising:

an issuer name;

a signature;

a holder name;

an attribute; and

an extension, wherein the extension comprises a locator identifying a location of a public key certificate of an issuing authority for the attribute certificate.